

# Penetration Testing

Keeping your business systems secure is imperative for data protection and client assurance. By regularly penetration testing your networks, both internally and externally, you could prevent breaches from occurring and increase security.

## Why should I implement pen testing?

When trying to decide whether penetration testing is right for your business, you must first ask yourself one key question.

*Would I rather have my system hacked by someone who will... maliciously use or steal my data?*

OR

*Use any weaknesses to help build on my existing security?*

Ethical hacking allows us to see how your current security measures up against the different types of cyber threats.

**A penetration test gives you the answers!!!**

## Made simple for you

Not only will MoCS keep you updated on the findings of your pen test, but we run everything for you. You won't have to do a thing until you receive those results.

## Complete testing package

Our penetration testing won't get in the way of your daily work. However, it will offer a comprehensive look into your existing security measures.

> [BOOK A CALL](#)

> [GET A QUOTE](#)

## Educate yourself on

Lack of knowledge can be a big weakness when it comes to cyber security. Educating yourself with the reports of your pen test could help to keep you one step ahead of cybercrime.

## Track your activities

An additional benefit of implementing regular penetration testing is that you can log and monitor all activity on your systems. This can give you more opportunity to detect potentially hazardous behaviours and act on any attempted entries before they become a problem.

## Tick those

Remaining compliant is essential for your clients to be able to trust you with their valuable data. Additional compliance measures could also make a big difference when your business becomes a target.





# How we do it

The Ministry of Cyber Security offers bespoke penetration testing dependent on your needs.

## All Tests Include:

### VALIDATION

You can check users' credentials for accuracy, as well as what they have access to. Having more knowledge of your teams credentials can massively improve security.

### FAKE TESTS

We will try to put fake, non-harmful viruses onto your devices to see how well your existing methods can highlight and repel them.

### SEEKING DATA

Use individual accounts to try and seek out sensitive information (such as personal or financial details) higher up the chain of command.

### OUTGOING INFO

External data can also be a risk. We will try to gain access to any data leaving your domain to see how easy it is to infiltrate.

## Futureproof your security

As hackers get smarter, so must you. Pen testing logs your activities and how they affect security. By detecting and acting on malicious activity, you may be better prepared to cope with any attacks on your system. This can include looking at how those attacks, and your preventative measures, change over time.

## GDPR compliance

It is your responsibility to ensure any confidential or sensitive data is adequately secured within your systems. As part of GDPR compliance, pen testing shows you have gone above and beyond to protect that information from malicious access or use.

[BOOK A CALL](#)

[GET A QUOTE](#)

## Assessment Capabilities

You get two different types of assessment within your pen testing. These will give you a comprehensive outlook into your network security.

### Inside your network

Discontent employees and human error can lead to security breaches from within your network. Assessing how secure your systems are for users can help to greatly mitigate these risks.

### Outside your network

Hackers may attempt to gain access to your information from across the world.

Our tests will see if there are any gaps in your security that unaffiliated individuals could use as footholds into your data.